Nama : Ewaldo Haryoseno Heditianto

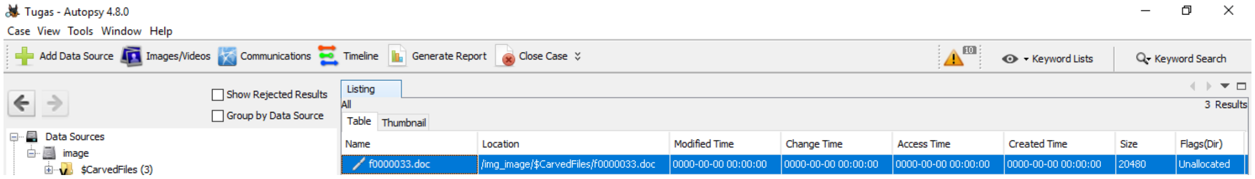
NIM : 09021181520001

TUGAS FORENSIK

a) Supplier Marijuana Jacob :

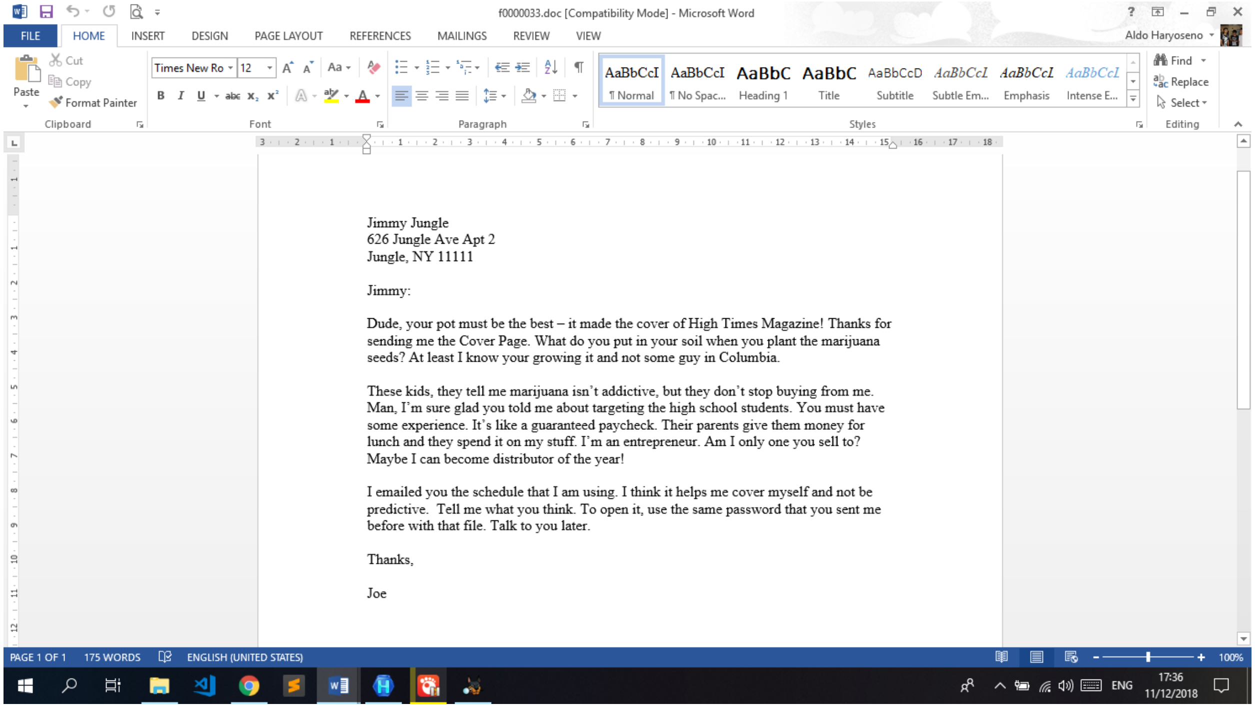
Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 111111

Bukti :
Dengan menggunakan autopsy ditemukan file “jimmyjungle.doc” yang dihapus oleh Jacob



Name	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)
f0000033.doc	/img_image/$CarvedFiles/f0000033.doc	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	20480	Unallocated

Adanya surat yang di hapus oleh Jacob suratnya adalah sebagai berikut



Jimmy Jungle
626 Jungle Ave Apt 2
Jungle, NY 11111

Jimmy:

Dude, your pot must be the best – it made the cover of High Times Magazine! Thanks for sending me the Cover Page. What do you put in your soil when you plant the marijuana seeds? At least I know your growing it and not some guy in Columbia.

These kids, they tell me marijuana isn’t addictive, but they don’t stop buying from me. Man, I’m sure glad you told me about targeting the high school students. You must have some experience. It’s like a guaranteed paycheck. Their parents give them money for lunch and they spend it on my stuff. I’m an entrepreneur. Am I only one you sell to? Maybe I can become distributor of the year!

I emailed you the schedule that I am using. I think it helps me cover myself and not be predictive. Tell me what you think. To open it, use the same password that you sent me before with that file. Talk to you later.

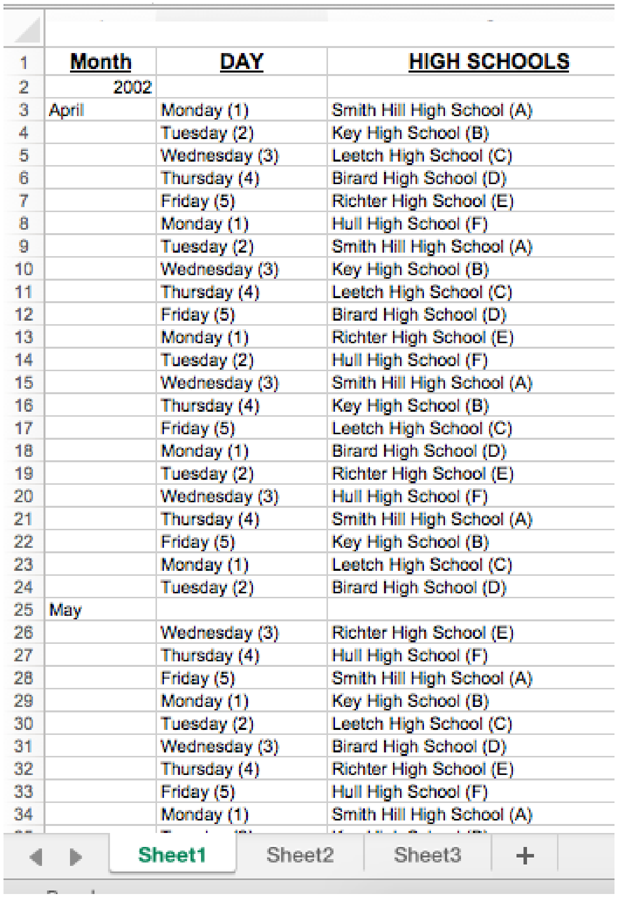
Thanks,

Joe

b) What crucial data is available within the coverpage.jpg file and why is this data crucial?

File, coverpage.jpg, berisi string pw = goodtimes yang tampaknya merupakan kata sandi. Kata sandi diperlukan untuk mendekripsi dan membuka file zip.

c) What (if any) other high schools besides Smith Hill does Joe Jacobs frequent?



1	Month	DAY	HIGH SCHOOLS
2	2002		
3	April	Monday (1)	Smith Hill High School (A)
4		Tuesday (2)	Key High School (B)
5		Wednesday (3)	Leetch High School (C)
6		Thursday (4)	Birard High School (D)
7		Friday (5)	Richter High School (E)
8		Monday (1)	Hull High School (F)
9		Tuesday (2)	Smith Hill High School (A)
10		Wednesday (3)	Key High School (B)
11		Thursday (4)	Leetch High School (C)
12		Friday (5)	Birard High School (D)
13		Monday (1)	Richter High School (E)
14		Tuesday (2)	Hull High School (F)
15		Wednesday (3)	Smith Hill High School (A)
16		Thursday (4)	Key High School (B)
17		Friday (5)	Leetch High School (C)
18		Monday (1)	Birard High School (D)
19		Tuesday (2)	Richter High School (E)
20		Wednesday (3)	Hull High School (F)
21		Thursday (4)	Smith Hill High School (A)
22		Friday (5)	Key High School (B)
23		Monday (1)	Leetch High School (C)
24		Tuesday (2)	Birard High School (D)
25	May		
26		Wednesday (3)	Richter High School (E)
27		Thursday (4)	Hull High School (F)
28		Friday (5)	Smith Hill High School (A)
29		Monday (1)	Key High School (B)
30		Tuesday (2)	Leetch High School (C)
31		Wednesday (3)	Birard High School (D)
32		Thursday (4)	Richter High School (E)
33		Friday (5)	Hull High School (F)
34		Monday (1)	Smith Hill High School (A)

Leetch High School, Birard High School, Richter High School, Key High School, dan Hull High School

d) For each file, what processes were taken by the suspect to mask them from others?

Jimmyjungle.doc -> dihapus
Cover page.jpgc - > sebenarnya merupakan file jpg
Scheduled visits.exe -> sebenarnya merupakan file zip yg dipassword yang didalamnya terdapat file xls.

e) What processes did you (the investigator) use to successfully examine the entire contents of each file?

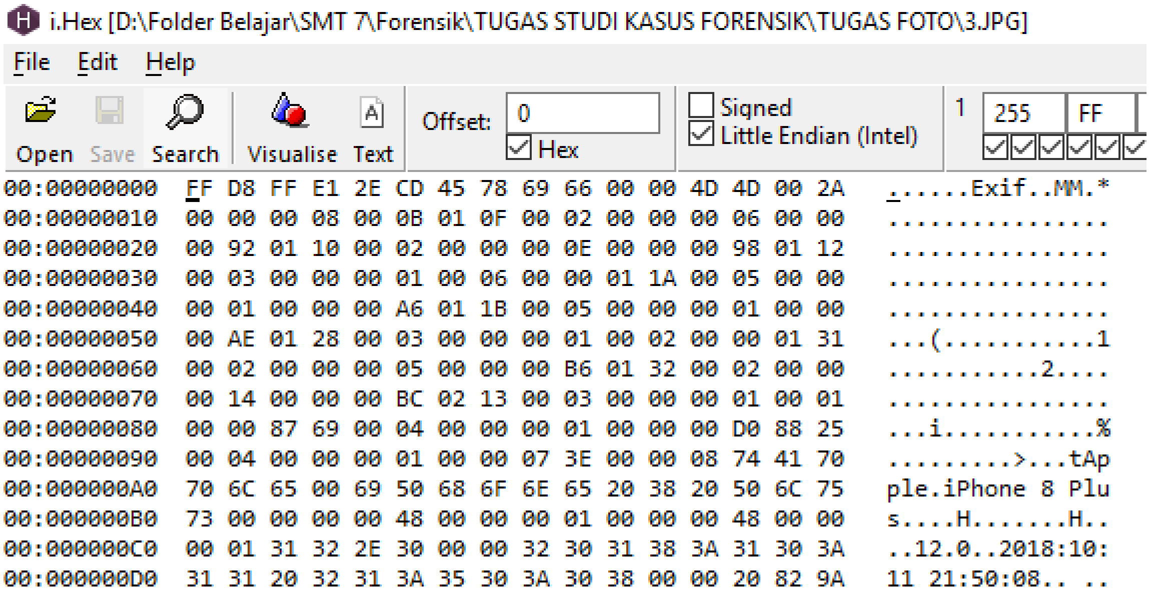
Proses yang saya lakukan adalah dengan menganalisa bukti yang ada dengan software autopsy, dari situ didapatkan 3 buah file yaitu :

Jimmyjungle.doc -> dihapus
Cover page.jpgc - > sebenarnya merupakan file jpg
Scheduled visits.exe -> sebenarnya merupakan file zip yg dipassword yang didalamnya terdapat file xls.

Kemudian membuka cover page.jpg dengan menggunakan ihex kemudian ditemukan password : goodtimes yang ternyata merupakan password dari file Scheduledvisits.zip yang berisi daftar tempat Jacob menjual Marijuananya.

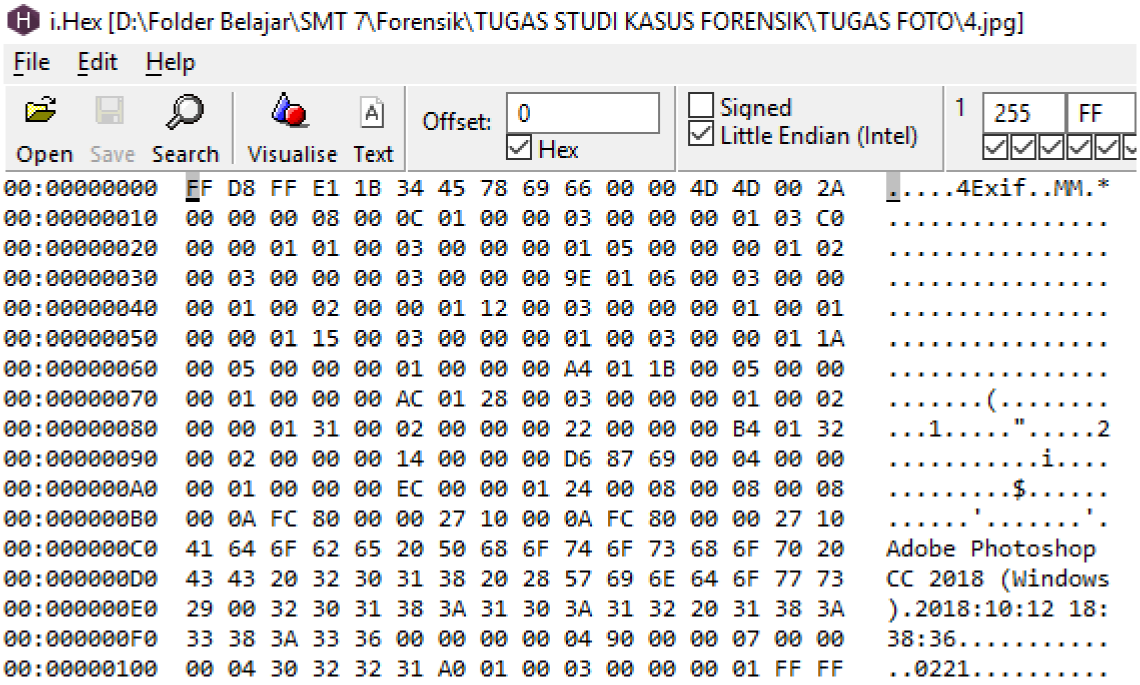
Soal Analisis Gambar :

Foto 3.jpg merupakan foto asli yang diambil menggunakan smartphone apple iPhone 8 Plus, pada tanggal 11 Oktober 2018, pada pukul 21:50:08.



```
00:00000000  FF D8 FF E1 2E CD 45 78 69 66 00 00 4D 4D 00 2A   ......Exif..MM.*
00:00000010  00 00 00 08 00 0B 01 0F 00 02 00 00 00 06 00 00   ................
00:00000020  00 92 01 10 00 02 00 00 00 0E 00 00 00 98 01 12   ................
00:00000030  00 03 00 00 00 01 00 06 00 00 01 1A 00 05 00 00   ................
00:00000040  00 01 00 00 00 A6 01 1B 00 05 00 00 00 01 00 00   ................
00:00000050  00 AE 01 28 00 03 00 00 00 01 00 02 00 00 01 31   ...(...........1
00:00000060  00 02 00 00 00 05 00 00 00 B6 01 32 00 02 00 00   ...........2....
00:00000070  00 14 00 00 00 BC 02 13 00 03 00 00 00 01 00 01   ................
00:00000080  00 00 87 69 00 04 00 00 00 01 00 00 00 D0 88 25   ...i...........%
00:00000090  00 04 00 00 00 01 00 00 07 3E 00 00 08 74 41 70   .........>...tAp
00:000000A0  70 6C 65 00 69 50 68 6F 6E 65 20 38 20 50 6C 75   ple.iPhone 8 Plu
00:000000B0  73 00 00 00 00 48 00 00 00 01 00 00 00 48 00 00   s....H.......H..
00:000000C0  00 01 31 32 2E 30 00 00 32 30 31 38 3A 31 30 3A   ..12.0..2018:10:
00:000000D0  31 31 20 32 31 3A 35 30 3A 30 38 00 00 20 82 9A   11 21:50:08.. ..
```

Foto 4.jpg merupakan foto yang telah di edit merupakan Adobe Photoshop CC 2018 pada tanggal 12 Oktober 2018 pada pukul 18:38:36.



```
00:00000000  FF D8 FF E1 1B 34 45 78 69 66 00 00 4D 4D 00 2A   .....4Exif..MM.*
00:00000010  00 00 00 08 00 0C 01 00 00 03 00 00 00 01 03 C0   ................
00:00000020  00 00 01 01 00 03 00 00 00 01 05 00 00 00 01 02   ................
00:00000030  00 03 00 00 00 03 00 00 00 9E 01 06 00 03 00 00   ................
00:00000040  00 01 00 02 00 00 01 12 00 03 00 00 00 01 00 01   ................
00:00000050  00 00 01 15 00 03 00 00 00 01 00 03 00 00 01 1A   ................
00:00000060  00 05 00 00 00 01 00 00 00 A4 01 1B 00 05 00 00   ................
00:00000070  00 01 00 00 00 AC 01 28 00 03 00 00 00 01 00 02   .......(........
00:00000080  00 00 01 31 00 02 00 00 00 22 00 00 00 B4 01 32   ...1.....".....2
00:00000090  00 02 00 00 00 14 00 00 00 D6 87 69 00 04 00 00   ...........i....
00:000000A0  00 01 00 00 00 EC 00 00 01 24 00 08 00 08 00 08   .........$......
00:000000B0  00 0A FC 80 00 00 27 10 00 0A FC 80 00 00 27 10   ......'.......'.
00:000000C0  41 64 6F 62 65 20 50 68 6F 74 6F 73 68 6F 70 20   Adobe Photoshop
00:000000D0  43 43 20 32 30 31 38 20 28 57 69 6E 64 6F 77 73   CC 2018 (Windows
00:000000E0  29 00 32 30 31 38 3A 31 30 3A 31 32 20 31 38 3A   ).2018:10:12 18:
00:000000F0  33 38 3A 33 36 00 00 00 00 04 90 00 00 07 00 00   38:36...........
00:00000100  00 04 30 32 32 31 A0 01 00 03 00 00 00 01 FF FF   ..0221..........
```